CLAIMS

What is claimed is:

1. A method comprising:

receiving first data to be blindly signed;

establishing parameter data for use with signature generating logic that encrypts data based on a Jacobian of at least one curve, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve;

determining private key data and corresponding public key data using said signature generating logic; and

generating second data by signing said first data with said private key data using said signature generating logic, said second data having a corresponding blind digital signature.

2. The method as recited in Claim 1, further comprising

generating said first data by:

digitally signing a message $m \in \{0, 1\}^*$,

determining $h=h(m) \in G$,

selecting a random $r \in Z_p^*$ and

setting $h' = r \cdot h' \in G$, wherein said first data includes h'.

3. The method as recited in Claim 2, wherein said parameter data establishes a base group G of order p and generator g as system parameters for said signature generating logic.

4. The method as recited in Claim 3, wherein determining said private key data and said public key data includes:

picking $x \overset{R}{\leftarrow} Z_p^*$, and

computing $v \leftarrow g^x$, wherein said public key data includes v and said private key data includes x.

5. The method as recited in Claim 4, wherein generating second data by signing said first data further includes:

signing h' by computing $\sigma' = x \cdot h' \in G$.

6. The method as recited in Claim 5, further comprising:

determining if said blind digital signature is valid.

7. The method as recited in Claim 6, wherein determining if said blind digital signature is valid further includes:

obtaining a GDH signature on h by computing $\sigma = r \cdot \sigma' \in G$ where $r' = r^{-1}$ mod p and $\sigma = x \cdot h \in G$ is a valid GDH signature on m; and

determining if (g, v, h, σ) is a valid Diffie-Hellman tuple

8. A computer-readable medium having computer-implementable instructions for performing acts comprising:

receiving first data to be blindly signed;

configuring signature generating logic using parameter data so as to be capable of encrypting data based on a Jacobian of at least one curve, said

parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve;

determining private key data and corresponding public key data using said signature generating logic; and

generating second data by signing said first data with said private key data using said signature generating logic, said second data having a corresponding blind digital signature.

9. The computer-readable medium as recited in Claim 8 having computer-implementable instructions for performing further acts comprising:

generating said first data by digitally signing a message $m \in \{0, 1\}^*$, determining $h=h(m) \in G$, selecting a random $r \in Z_p^*$ and setting $h'=r \cdot h' \in G$, wherein said first data includes h'.

10. The computer-readable medium as recited in Claim 9, wherein said parameter data establishes a base group G of order p and generator g as system parameters for said signature generating logic.

11. The computer-readable medium as recited in Claim 10, wherein determining said private key data and said public key data further includes:

picking $x \in_R Z_p^*$, and

computing $v \leftarrow g^x$, wherein said public key data includes v and said private key data includes x.

12. The computer-readable medium as recited in Claim 11, wherein generating second data by signing said first data further includes:

signing h' by computing $\sigma' = x \cdot h' \in G$.

13. The computer-readable medium as recited in Claim 12, having computer-implementable instructions for performing further acts comprising:

determining if said blind digital signature is valid.

14. The method as recited in Claim 13, wherein determining if said blind digital signature is valid further includes:

obtaining a GDH signature on h by computing $\sigma = r \cdot \sigma' \in G$ where $r' = r^{-1}$ mod p and $\sigma = x \cdot h \in G$ is a valid GDH signature on m; and

determining if (g, v, h, σ) is a valid Diffie-Hellman tuple

15. An apparatus comprising:

memory configured to store first data that is to be blindly signed; and

signature generating logic operatively coupled to said memory and configured according to parameter data so as to be capable of encrypting data based on a Jacobian of at least one curve, said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve, determine private key data and corresponding public key data, and generate second data by signing said first data with said private key data, said second data having a corresponding blind digital signature.

16. The apparatus as recited in Claim 15 wherein said first data is generated by a second logic operatively coupled to said first logic by digitally signing a message $m \in \{0, 1\}^*$, determining $h=h(m) \in G$, selecting a random $r \in Z_p^*$ and setting $h'=r \cdot h' \in G$, wherein said first data includes h'.

17. The apparatus as recited in Claim 16, wherein said parameter data establishes a base group G of order p and generator g as system parameters for said signature generating logic.

18. The apparatus as recited in Claim 17, wherein said signature generating logic is further configured to determine said private key data and said public key data by picking $x \in_R Z_p^*$, and computing $v \leftarrow g^x$, wherein said public key data includes v and said private key data includes x.

19. The apparatus as recited in Claim 18, wherein said signature generating logic is further configured to generate said second data by signing h' and computing $\sigma' = x \cdot h' \in G$.

20. The apparatus as recited in Claim 15, wherein said memory and said signature generating logic are provided within a computing device.